REMARKS

An Examiner interview was conducted on October 6, 2008.

IDS ACKNOWLEDGEMENT

Consideration and Acknowledgement of the IDS of June 8, 2007 is requested. Along with a Communication to the Examiner filed March 27, 2008, another copy of the citations were resubmitted on March 27, 2008. Further, consideration and acknowledgment of the IDS of March 28, 2008 is requested.

REJECTIONS

Claims 6, 8-21 and 23-31 are pending.

Claims 6, 8-21 and 23-31 are rejected under 35 USC 112, second paragraph, for indefiniteness as indicated.

Claim 10's "device parameter" is definite and complies with 35 USC 112, second paragraph, because the metes and bound or scope of the phrase 'parameter' is clear to one skilled in the art, namely any variable or argument associated with the device. MPEP 2173.04 expressly guides that breadth of a claims is not to be equated with indefiniteness.

Claims 6, 8-21 and 23-31 are rejected under 35 USC 112, first paragraph, for failing to comply with the written description requirement. Paragraph 487 expressly supports the claims as amended. As discussed in the interview, regarding the language 'first view of the agreement …, a second view of the agreement …' for example, FIG. 31 expressly illustrates the consumer message as the first view of the agreement and a merchant message as the second view of the agreement. Withdrawal of the rejection is requested.

Claims 6, 8-21 and 23-31 are rejected under 35 USC 101 and 112, second paragraph, for allegedly overlapping two different statutory classes. The claims are amended.

Claim 10 is rejected on the ground of non-statutory obviousness-type double patenting over US Patent No. 7,349,871.

Claims 8-10 and 14-19 are rejected under 35 USC 103(a) as being unpatentable over Slater (US Patent No. 6,098,093) and Hurst (2003-0226030).

Claims 11 and 13 are rejected under 35 USC 103(a) as being unpatentable over Slater, Hurst and in view of Kuroda (US Patent No. 6,470,448).

Claims 6, 12, 20, 21, 23-25, 29 and 31 are rejected under 35 USC 103(a) as being unpatentable over Slater, Hurst, Kuroda and Husemann (US Publication No. 2001/0037264).

The independent claim is 10, which is rejected as being obvious over Slater and Hurst.

Slater discusses DES and Hurst discusses deriving a key based upon a stored secret key and a stored memory device identifier (column 8, claim 7 and paragraph s 46-47). Slater's DES differs from the claimed symmetric agreement verification protocol, because Slater column 8, lines 14-16 only discusses a conventional DES in which the financial institution 22 holds the decryption key. However, the language of the claims provides "a key derived from ~~based upon~~ both a first mobile device parameter stored in the mobile device and input personal identifying information of the first party as a second input mobile device parameter input to the mobile device."

Further, for the claimed mobile device parameters, the Office Action relies upon Slater column 7, lines 66-67 and column 8, lines 1-28, and column 9, lines 809, however, Slater only discusses using the PIN 'by a cardholder to identify themselves to their bank to authorize on-line ATM/POS transaction,' and Slater column 8, lines 17-21 expressly discuss 'Card reader device 64 forwards the encrypted card information 39 and security information 40 [i.e., PIN] (column 7, lines 60-63) to computer 50, …" So Slater expressly discusses encrypting both the card information 39 and security information 40 and transmitting the encrypted card information 39 and security information 40.

Therefore, Slater fails to expressly or implicitly disclose to one skilled in the art to be modified to provide the claimed "***generating … a first view*** of the agreement and ***securing the first view*** of the agreement ***based upon ~~secured by~~ a key derived from ~~based upon~~ both a first mobile device parameter stored in the mobile device and input personal identifying information of the first party as a second input mobile device parameter input to the mobile device*** and transmitting the first view of the agreement to the second party***, the first view of the agreement not including the first and second mobile device parameters***." In other words, Slater's card information 39 and security information 40 [i.e. PIE] cannot correspond to both the claimed "first view of the agreement" and the first and second mobile device parameters, since Slater expressly discusses encrypting both the card information 39 and security information 40 and transmitting the encrypted card information 39 and security

information 40. So in Slater the card information 39 and security information 40 would be part of the transmitted agreement.

Further, in Slater, both the card information 39 and the security information 40 are input via the card 44, whereas the language of the claims only provides for one of the mobile device parameters to be input.

Further, for key derivation, the Office Action relies upon Hurst, however, Hurst paragraph 47 and Hurst claim 7, as illustrated by FIG. 4, discuss deriving a key from a hidden secret key 424 and a memory device identifier 426, both of which are stored. In other words, Hurst discusses unlocking the SSC 420 of the MultiMedia Card (MMC) based upon a stored hidden key 424 and stored MMC ID 426, so Hurst is silent on an input mobile device parameter. However, the language of claims expressly provides "***generating*** … ***a first view*** of the agreement and ***securing the first view of the agreement based upon*** ~~***secured by***~~ ***a key derived from*** ~~***based upon***~~ ***both a first mobile device parameter stored in the mobile device and input personal identifying information of the first party as a second input mobile device parameter*** input to the mobile device and transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameters***."

Further, Hurst paragraph 47 and claim 7, as illustrated by FIG. 4, expressly discuss the derived key based upon both the key 424 and the MMC ID 426 are used to unlock the Secured Content Container (SCC) 420, which is located on the MultiMedia Card (MMC). In other words, Hurst does not use the derived key to provide the claimed "***securing the first view of the agreement based upon*** ~~***secured by***~~ ***a key derived from*** ~~***based upon***~~ ***both a first mobile device parameter stored in the mobile device and input personal identifying information of the first party as a second input mobile device parameter***."

Further, Hurst is silent on and fails to suggest, expressly or implicitly, conducting an agreement between parties using a mobile device, since Hurst only discusses using its derived key for activating protected content on a portable memory device of the mobile terminal (Abstract, FIG. 4, paragraphs 46-47).

Further, both Slater and Hurst are silent on the claimed "***trusted third party server*** … ***verifying*** ~~***verifies***~~ ***conditions of the agreement*** … based upon ***… deriving the key based upon the first and second mobile device parameters for the secured first view and using***

the first and second merchant device parameters for the secured second view," because as acknowledged by the Office Action, Slater is silent on the claimed key derivation, and further, Hurst does not conduct an agreement between parties involving the mobile terminal.

In other words, the Office Action alleges that Slater discusses a first and a second parameter, namely the card information 39 and the security information 40, which are encrypted by a key and transmitted, and that Hurst discusses deriving a key from two parameters, which can be combined with Slater for encrypting Slater's first and second parameters. However, the combination of Slater and Hurst teaches away from the present invention or would result in a very weak encryption method (unsecure). Because, if as the examiner alleges one could use Hurst to derive a key from first and second parameters of Slater, namely the card information 39 and the security information 40 [i.e., PIN], and then use that key to encrypt and transmit both the encrypted first and second parameters, namely transmit the encrypted card information 39 and the security information 40 [i.e., PIN], aside from the fact that the language of the claims only requires using the derived key for "***securing the first view of the agreement*** … ***the first view of the agreement not including the first and second mobile device parameters***," a problem would be that the first and second parameters would be encrypted with a key derived from the first and second parameters. It is submitted this could be a very weak encryption method (might be unsecure), because the derived key is also used to encrypt itself (i.e., the first and second parameters) which can make successful attacks faster than a brute force attack (trying all possible keys), since the plaintext (first and second parameters) is also present in the key that is used to encrypt it.

Thus, it is submitted that one skilled in the art would not use the Hurst method to derive a key from first and second parameters and then encrypt the first and second parameters with the derived key (combined Slater and Hurst), because this would result to very weak security. In other words, Slater's card information 39 and security information 40 [i.e. PIE] cannot correspond to both the claimed "first view of the agreement" and the first and second mobile device parameters, since the language of claim 10 provides "***generating*** … ***a first view*** of the agreement ***and securing the first view of the agreement based upon ~~secured by~~ a key derived from ~~based upon~~ both a first mobile device parameter stored in the mobile device and input personal identifying information of the first party as a second input mobile device parameter*** … and transmitting the first view of the agreement to the second party***, the first view of the agreement not including the first and second mobile device parameters***."

Further, nothing has been cited or found that one skilled in the art would further modify the combination of Slater and Hurst to achieve the language of the claims, namely a prima facie case of obviousness based upon Slater and Hurst cannot be established, because nothing has been cited or found that Hurst expressly or implicitly discloses to one skilled in the art to combine Hurst with Slater and then further modify Hurst's key derivation for unlocking the SCC 420 to include "***input personal identifying information of the first party as a second input mobile device parameter***," and then even further modify Hurst's mobile terminal to provide the claimed conducting an agreement between parties and even further modify Slater's discussion of using the PIN 'by a cardholder to identify themselves to their bank to authorize on-line ATM/POS transaction,' and Slater's column 8, lines 17-21 discussion of 'Card reader device 64 forwards the encrypted card information 39 and security information 40 [i.e., PIN] to computer 50, …', to provide the claimed "***securing the first view of the agreement based upon ~~secured by~~ a key derived from ~~based upon~~ both a first mobile device parameter stored in the mobile device and input personal identifying information of the first party as a second input mobile device parameter … the first view of the agreement not including the first and second mobile device parameters***," in combination with other claimed features, namely "***open and non-secure wireless network***," and "***trusted third party server verifying conditions of the agreement … based upon … deriving the key based upon the first and second mobile device parameters for the secured first view and using the first and second merchant device parameters for the secured second view***," and "wherein ***only the STS stores … the ~~input~~ second input mobile device parameter***," and seen the following benefits:

> A benefit of the embodiments is to substantially reduce the risk of unauthorized derivation of the key, because only one of the parameters based upon which the key is derived is stored in the mobile device and the other second parameter is ***input***, namely "***input personal identifying information of the first party as a second input mobile device parameter*** input to the mobile device." So even if the mobile device is lost or used by other than the user, an agreement and/or the key cannot be conducted/derived without the "***second input mobile device parameter***." And even if the first view is intercepted, it is very difficult to reverse engineer the first and second parameters, because of "***the first view of the agreement not including the first and second mobile device parameters***."
>
> Another benefit is that a secure channel in wireless communication environment may or may not be used according to application criteria, for example, if desired to avoid pre-arrangement, or in case of SSL, speed wireless communication

and/or not require key distribution, management and storage at wireless mobile device, which might not practical from a usability perspective (see paragraphs 239 and 478-479 of the present application).

Withdrawal of the rejection of independent claim 10 and allowance of claim 10 is requested.

Dependent claims recite patentably distinguishing features of their own or are at least patentably distinguishing due to their dependencies from the independent claim 10.

It is believed, the claims are now in condition for allowance, which is respectfully requested.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

Date: December 24, 2008

By: /Mehdi D. Sheikerz/
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501